UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,852	12/21/2001	Paul Nicholas Gartside	01.122.01	5732

7590 09/22/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
BESROUR, SAOUSSEN	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,852	GARTSIDE ET AL.	
	Examiner	Art Unit	
	Saoussen Besrour	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *4/13/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8-17,19-22,24-33,35-38 and 40-47* is/are pending in the application.

4a) Of the above claim(s) *2, 7, 18, 23, 39 and 48* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-17,19-22,24-33,35-38 and 40-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to amendment filed 4/13/2006. Claims 1, 17 and 33 were amended. Claims 2, 7, 18, 23, 39 and 48 were cancelled. Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/17/2006 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claim 1, 10, 17 and 33** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claims 1, 17 and 33**, the limitation " said fixed location computing device may transfer computer files and corresponding threat data..." is indefinite because it is not clear whether the step of "transfer computer files and corresponding threat data..." takes place or not. Examiner suggests removing "may".

As per **claim 10**, the limitation "may transfer computer files ..." is indefinite because it is not clear whether the step of "transfer computer files..." takes place or not. Examiner suggests removing "may".

Claims 3-6, 8-16,19-22, 24-32, 35-38 and 40-47 are also rejected because they incorporate matter of their base claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahti et al. et al. (U.S. Pub. No. 2002/0042886) in view of Hypponen et al (U.S. patent No. 6,577,920).

As per **claim 1**, Lahti et al. et al. discloses: generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device (Paragraph 6); generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (Paragraph 3, Paragraph 5, lines 1-9 and Paragraph 6); wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (Paragraph 23, Lines 4-8). Lahti et al. does not explicitly teach obtaining code operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat; identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data; wherein one a subset of master malware definition data is used to generate said mobile computing

device malware definition data for tailoring said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable; wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies. However, Hypponen discloses: obtaining code operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat (Column 2, Lines 27-39); identifying code operable to identify one or more classes of malware (blocking transfer of unidentified macros) threat against which said mobile computing device is to be protected (Column 2, Lines 37-44); and wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (Column 2, Lines 47-63); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate (update) only malware threats to which said mobile computing devices is vulnerable (Column 2, Lines 27-63); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile

computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (Column 2, lines 55-63 and Column 3, Lines 3-14). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Hypponen in conjunction with the teachings of Lahti et al. et al. for the benefit of blocking transfer of and processing of files which contain a previously unidentified macros virus (Column 2, Lines 42).

As per **claim 17**, Lahti et al. et al. discloses: generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device (Paragraph 6); generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (Paragraph 3, Paragraph 5, lines 1-9 and Paragraph 6); wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (Paragraph 23, Lines 4-8). Lahti et al. does not explicitly teach obtaining from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality

of classes of malware threat; identifying one or more classes of malware threat against which said mobile computing device is to be protected; and wherein said steps of obtaining, identifying and generating are performed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data; wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable; wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies. However, Hypponen discloses: obtaining from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat (Column 2, Lines 27-39); identifying one or more classes of malware (blocking transfer of unidentified macros) threat against which said mobile computing device is to be protected (Column 2, Lines 37-44); and wherein said steps of obtaining, identifying and said generating are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (Column 2, Lines 47-

63); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate (update) only malware threats to which said mobile computing devices is vulnerable (Column 2, Lines 27-63); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (Column 2, lines 55-63 and Column 3, Lines 3-14). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Hypponen in conjunction with the teachings of Lahti et al. et al. for the benefit of blocking transfer of and processing of files which contain a previously unidentified macros virus (Column 2, Lines 42).

As per **claim 33**, Lahti et al. et al. discloses: generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device (Paragraph 6); generating logic operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (Paragraph 3, Paragraph 5, lines 1-9 and Paragraph 6); wherein said fixed

location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (Paragraph 23, Lines 4-8). Lahti et al. does not explicitly teach obtaining logic operable to obatin from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat; identifying logic operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and wherein said steps of obtaining, identifying and generating are performed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data; wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable; wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies. However, Hypponen discloses: obtaining logic operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware

each belonging to one of a plurality of classes of malware threat (Column 2, Lines 27-39); identifying logic operable to identify one or more classes of malware (blocking transfer of unidentified macros) threat against which said mobile computing device is to be protected (Column 2, Lines 37-44); and wherein said steps of obtaining, identifying and said generating are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (Column 2, Lines 47-63); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate (update) only malware threats to which said mobile computing devices is vulnerable (Column 2, Lines 27-63); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (Column 2, lines 55-63 and Column 3, Lines 3-14). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Hypponen in conjunction with the teachings of Lahti et al. et al. for the benefit of blocking transfer of and processing of files which contain a previously unidentified macros virus (Column 2, Lines 42).

As per **claims 3, 19 and 35**, rejected as applied to claims 1, 17 and 33. furthermore Lahti et al. discloses: said fixed location computing device is a user computer having communication link with said mobile computing device (Paragraph 23).

As per **claims 4, 20 and 36**, Rejected as applied to claims 1, 17 and 33. Furthermore Lahti et al. discloses: when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer filed respectively stored by said mobile computing device and said fixed location computing device are synchronized (Paragraph 23, Lines 1-7).

As per **claims 5, 21 and 37**, rejected as applied to claims 4, 20 and 36. Furthermore, Lahti et al. et al. discloses: said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization (Paragraph 23, Lines 1-7).

As per **claims 6, 22 and 38**, rejected as applied to claims 4, 20 and 36. Furthermore, Lahti et al. discloses: when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device (Paragraph 23, Paragraph 25-27).

As per **claim 8, 24 and 40**, rejected as applied to claims 1, 17 and 33. Furthermore, Lahti et al. et al. discloses: wherein user controlled policy data us used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data (Paragraph 21, Lines 7-10).

As per **claims 9, 25 and 41**, rejected as applied to claims 1, 17 and 33. Furthermore, Lahti et al. discloses: different types of operating system computer program used by mobile computing device (Paragraph 13).

As per **claim 10, 26 and 42**, rejected as applied to claims 1, 17 and 33. Furthermore, Lahti et al. et al. discloses: said fixed location computer device detects to which mobile computing devices it may transfer computer files by detecting installation upon fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices (Paragraph 15, Paragraph 23, Lines 1-8).

As per **claim 11, 27 and 43**, rejected as applied to claims 1, 17 and 33. Furthermore, Lahti et al. discloses: fixed location computing device also transfers a malware scanner computer program from said data source to said mobile device (Paragraph 2).

As per **claim 12**, rejected as applied claims 1, 17 and 33. Furthermore, Lahti et al. discloses said fixed location computing device checks for updated master malware definition data becoming available from said data source, if such updated master

malware definition become available, then repeats steps of obtaining, identifying and generating (Paragraph 23, Lines 1-7).

As per **claim 13, 29 and 45**, rejected as applied to claim 11, 27 and 43. Furthermore, Lahti et al. discloses: said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an update malware scanner computer program becomes available, then obtains said updated malware scanner computer program for transfer to said mobile computing device (Paragraph 27).

As per **claim 14, 30 and 46**, rejected as applied to claim 1, 17, 33. Furthermore, Lahti et al. et al, discloses: said master malware definition is data also used to protect said fixed location computing device from malware (Paragraph 70.

As per **claim 15 and 31**, rejected as applied to claims 1 and 17. Furthermore, Lahti et al. discloses: said fixed location computing device is connected to said data source by a fixed interner link (Paragraph 23).

As per **claims 16 and 32**, rejected as applied to claims 1 and 17. Furthermore, lathi et al discloses: said item of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (Paragraph 3).

As per **claim 47**, rejected as applied to claim 1. Furthermore, Lahti et al. discloses: said fixed location device stores policy data including user defined settings identifying the manner in which said profile data is to be intercepted (23, Lines 7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrour whose telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
September 16, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/18/06